PCT/AU03/00934

10752067

REC'D 07 AUG 2003
WIPO PCT

Rec'd PCT/PTO 21 JAN 2005
PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

AU03/00934

Patent Office
Canberra

I, KARYN DUNNE, MANAGER AUSTRALIAN RECEIVING OFFICE, hereby certify that the annexed is a true copy of International Application PCT/AU02/00984 filed at the Australian Receiving Office on 24 July 2002.

BEST AVAILABLE COPY

WITNESS my hand this
Twenty-eighth day of July 2003

KARYN DUNNE
MANAGER
AUSTRALIAN RECEIVING OFFICE

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/AU 02/00984

International Application No.

24 JUL 2002 (24.7.2002)

International Filing Date

Australian Patent Office
PCT INTERNATIONAL APPLICATION

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* 595897C

Box No. I TITLE OF INVENTION

Biometric Smartcard System and Method of Secure Transmission

Box No. II APPLICANT ☐ This person is also inventor.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)*

BANQUE-TEC INTERNATIONAL PTY LTD
Unit 5, 12-18 Victoria Street East
Lidcombe, NSW 2141
AUSTRALIA

Telephone No.
(02) 9749 4999

Facsimile No.
(02) 9749 5100

Teleprinter No.

Applicant's registration No. with the Office

State *(that is, country)* of nationality:
Australia

State *(that is, country)* of residence:
Australia

This person is applicant for the purposes of : ☐ all designated States ☒ all designated States except the United states of America ☐ the United states of America only ☐ The States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)*

BLAKE, Christopher Ian
c/o Banque-Tec International
Unit 5, 12-18 Victoria Street
East Lidcombe, NSW 2141
AUSTRALIA

This person is :
☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:
Australia

State *(that is, country)* of residence:
Australia

This person is applicant for the purposes of : ☐ all designated States ☐ all designated States except the United states of America ☒ the United states of America only ☐ The States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as : ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country)*

SPRUSON & FERGUSON
GPO BOX 3898
Sydney
New South Wales 2001
AUSTRALIA

Telephone No.
+61 2 9207 0777

Facsimile No.
+61 2 9232 8555

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Box No. V DESIGNATION OF STATES *Mark the applicable check-boxes; at least one must be marked.*

The following designations are hereby made under Rule 4.9(a):

Regional Patent

- ☒ **AP** **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☒ **EA** **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ **EP** **European Patent:** AT Austria, BE Belgium, BG Bulgaria, CH & LI Switzerland and Liechtenstein, CY Cyprus, CZ Czech Republic, DE Germany, DK Denmark, EE Estonia, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden , SK Slovakia, TR Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☒ **OA** **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GQ Equatorial Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)*

.....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

☒ AE United Arab Emirates	☒ GM Gambia	☒ NZ New Zealand
☒ AG Antigua and Barbuda	☒ HR Croatia	☒ OM Oman
☒ AL Albania	☒ HU Hungary	☒ PH Philippines
☒ AM Armenia	☒ ID Indonesia	☒ PL Poland
☒ AT Austria	☒ IL Israel	☒ PT Portugal
☒ AU Australia	☒ IN India	☒ RO Romania
☒ AZ Azerbaijan	☒ IS Iceland	☒ RU Russian Federation
☒ BA Bosnia and Herzegovina	☒ JP Japan	
☒ BB Barbados	☒ KE Kenya	☒ SD Sudan
☒ BG Bulgaria	☒ KG Kyrgyzstan	☒ SE Sweden
☒ BR Brazil	☒ KP Democratic People's Republic of Korea	☒ SG Singapore
☒ BY Belarus		☒ SI Slovenia
☒ BZ Belize	☒ KR Republic of Korea	☒ SK Slovakia
☒ CA Canada	☒ KZ Kazakhstan	☒ SL Sierra Leone
☒ CH & LI Switzerland and Liechtenstein	☒ LC Saint Lucia	☒ TJ Tajikistan
☒ CN China	☒ LK Sri Lanka	☒ TM Turkmenistan
☒ CO Colombia	☒ LR Liberia	☒ TN Tunisia
☒ CR Costa Rica	☒ LS Lesotho	☒ TR Turkey
☒ CU Cuba	☒ LT Lithuania	☒ TT Trinidad and Tobago
☒ CZ Czech Republic	☒ LU Luxembourg	
☒ DE Germany	☒ LV Latvia	☒ TZ United Republic of Tanzania
☒ DK Denmark	☒ MA Morocco	☒ UA Ukraine
☒ DM Dominica	☒ MD Republic of Moldova	☒ UG Uganda
☒ DZ Algeria		☒ US United States of America
☒ EC Ecuador	☒ MG Madagascar	
☒ EE Estonia	☒ MK The former Yugoslav Republic of Macedonia	☒ UZ Uzbekistan
☒ ES Spain		☒ VN Viet Nam
☒ FI Finland	☒ MN Mongolia	☒ YU Yugoslavia
☒ GB United Kingdom	☒ MW Malawi	☒ ZA South Africa
☒ GD Grenada	☒ MX Mexico	☒ ZM Zambia
☒ GE Georgia	☒ MZ Mozambique	☒ ZW Zimbabwe
☒ GH Ghana	☒ NO Norway	

Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:

☐	☐	☐ .....
☐	☐	☐ .....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)

Box No. VI PRIORITY CLA

Filing date of earlier application *(day/month/year)*	Number of earlier application	Where earlier application is:		
		national application: country or Member of WTO	regional application:* regional Office	international application: receiving Office
Item (1)				

☐ Further priority claims are indicated in the Supplemental Box.

☐ The receiving Office is hereby requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as item(s) : _____

** Where the earlier application is an ARIPO application, please indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):*

.....

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(If two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):*

ISA/ AU

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*

Date (day/month/year)	Number	Country (or regional Office)

Box No VIII DECLARATIONS

The following **declarations** are contained in Boxes Nos VIII(I) to (v) (*mark the applicable*

			Number of declarations
☐	Box No. VIII(i)	Declaration as to the identity of the inventor :	
☐	Box No VIII(ii)	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent :	
☐	Box No VIII(iii)	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application :	
☐	Box No VIII(iv)	Declaration of inventorship (only for the purposes of the designation of the United States of America) :	
☐	Box No VIII(v)	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty :	

INSERTED
RO/AU

Box No. IX CHECK LIST; LANGUAGE OF FILING

This international application contains:

(a) the following number of **sheets in paper form:**

request (including declaration sheets)	:	4
description (excluding sequence listing part)	:	14
claims	:	3
abstract	:	1
drawings	:	7
Sub-total number of sheets	:	29
sequence listing part of description *(actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see(b) below)*	:	
Total number of sheets	:	29

(b) sequence listing part of description filed in **computer readable form**

(i) ☐ only (under Section 801(a)(i))

(ii) ☐ in addition to being filed in paper form (under Section 801(a)(ii))

Type and number of carriers (diskette, CD-ROM, CD-R or other) on which the sequence listing part is contained *(additional copies to be indicated under item 9(ii), in right column):*

This international application is accompanied by the following item(s) (mark the applicable check-boxes below and indicate in right column the number of each item):

	Number of items
1. ☒ fee calculation sheet	1
2. ☐ original separate signed power of attorney	
3. ☐ original general power of attorney	
4. ☐ copy of general power of attorney; reference number, if any:	
5. ☐ statement explaining lack of signature	
6. ☐ priority document(s) identified in Box No. VI as item(s):	
7. ☐ translation of international application into (*language*):	
8. ☐ separate indications concerning deposited microorganism or other biological material	
9. ☐ sequence listing in computer readable form (indicate also type and number of carriers (diskette, CD-ROM, CD-R or other):	
(i) ☐ copy submitted for the purposes of international search under Rule 13*ter* only (and not as part of the international application)	
(ii) ☐ (*only where check-box (b)(i) or (b)(ii) is marked in left column*) additional copies including, where applicable, the copy for the purposes of international search under Rule 13*ter*	
(iii) ☐ together with relevant statement as to the identity of the copy or copies with the sequence listing part mentioned in left column	
10. ☐ other *(specify)*:	

Figure of the drawings which should accompany the abstract:

Language of filing of the international application: English

Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Scott Berggren
Registered Patent Attorney
SPRUSON & FERGUSON

For receiving Office use only

1.	Date of actual receipt of the purported international application: 24 JUL 2002 (24.7.2002)		
3.	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		2. Drawings
4.	Date of timely receipt of the required corrections under PCT Article 11(2):		☐ received:
5.	International Searching Authority (if two or more are competent): ISA/	6. ☐ Transmittal of search copy delayed until search fee is paid	☐ not received:

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

BIOMETRIC SMARTCARD SYSTEM AND METHOD OF SECURE TRANSMISSION

Field of the Invention

The present invention relates generally to security systems and in particular to secure transmission systems and security systems utilising biometric sensors.

Background

Existing security systems are of several different types. One type of security system utilises a smartcard as a key for access to a secure location or secure equipment. The smartcard contains security information providing access via a smartcard reader at the access point. A user presents the reader with the smartcard. If the smartcard is authorised, the reader actuates a control mechanism to provide access. Thus, for example, the reader may signal a controller that controls operation of a latch mechanism controlling access to a door or provide access to a computer terminal. One example of a relevant reader that may be used in such a system is a Wiegand reader. One significant disadvantage of such systems is that the smartcard if stolen or otherwise in the possession of an unauthorised person may allow the unauthorised person to access the secure location or equipment.

Another security system utilises a biometric sensor to control access. A user must provide biometric data, normally a fingerprint, speech, or an eye scan via a sensor at the access point. Other forms of biometric data include facial details and hand geometry. Biometrics is a physical characteristic of a person used as a form of identification. The biometrics data is used in place of, or in addition to a security key, such as a key, card or PIN. A database or central repository of stored biometric data is maintained in a computer, with which the sensor can communicate. The scanned biometric data is compared with the stored biometric data, and if a match is found the user is permitted access. This system is generally more secure than that of the smartcard system, but is disadvantageous in that a central repository of biometric data must be maintained and updated. Further, significant time may be required to conduct such a comparison of the scanned biometric data against the database or central repository to determine whether or not there is a match.

Conventional systems are also disadvantageous in that the products' sizes are bulky. Still a further disadvantage of conventional systems is that such products cannot protect against security breaches arising from a person getting into security lines in a wall to which the reader is connected and providing false authorisation signals and the like to a controller.

Summary

In accordance with a first aspect of the invention, identification using of biometric data is disclosed. A smartcard encoded with biometric data is read. Actual biometric data is sensed. The biometric data from the smartcard is then compared with the sensed biometric data for verification. Access may be allowed if the biometric data from the smartcard and the sensed biometric data match. This may involve verifying that the biometric data encoded on the smartcard is correct. The biometric data stored in the smartcard is derived by scanning a source of biometric data associated with the smartcard, encoding the scanned biometric data, and storing the encoded biometric data on the smartcard. The biometric data may include a fingerprint. Optionally, a detail level can be specified for scanning the biometric data.

In accordance with a second aspect of the invention, a method of providing secure transmissions from a reader is disclosed. A signal created by the reader is encrypted. The encrypted signal is transmitted to a remote location relative to the reader. At the remote location, the transmitted signal is translated to another format usable by a controller. Access is controlled using the controller dependent upon the translated signal.

Brief Description of the Drawings

A small number of embodiments are described hereinafter with reference to the drawings, in which:

Fig. 1 is a high-level flow diagram illustrating an enrolment operation of a biometric smartcard system including a biometric smartcard reader or encoder in accordance with an embodiment of the invention;

Fig. 2 is a flow diagram illustrating a process of enrolling a fingerprint on a smartcard using a biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 3 is a flow diagram illustrating a process of verifying a finger on the biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 4A is a block diagram illustrating the structure of storage or memory in a smartcard in accordance with the embodiment of the invention;

Fig. 4B is a table illustrating an arrangement of security keys used in the smartcard of Fig. 4A in accordance with the embodiment of the invention;

Fig. 5 is a functional block diagram showing modules of a biometric smartcard reader or encoder in accordance with the embodiment of the invention;

Fig. 6 is a perspective view of a biometric smartcard reader or encoder in accordance with the embodiment of the invention shown in Fig. 5;

Fig. 7 is a block diagram of a secure transmission system in accordance with a further embodiment of the invention; and

Fig. 8 is a flow diagram illustrating a process of secure transmission in accordance with the further embodiment of the invention, which may be practiced with the system of Fig. 7.

Detailed Description

A method, an apparatus, and a system for biometric smartcard reading and encoding, as well as for secure transmissions are described hereinafter. Numerous specific details are set forth. However, it will be apparent to those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention. Embodiments of the invention provide equipment that synthesise biometric and smartcard technologies to provide a smartcard reader or encoder that eliminates central database communications infrastructure. As the smartcard holds the biometric information, the requirement of central repositories of biometric data and associated security issues are obviated. A significant application of the reader or encoder is as an access control device at security point, whether for access via a door or other portal, or to a computer, network, or other secure equipment or installation.

In the following description, the terms biometric smartcard reader and biometric smartcard encoder are used. A reader is a device that is able to scan a person's biometric data and contactlessly read a smartcard to obtain stored biometric data. The biometric data is preferably a fingerprint. The smartcard is presented to the reader (preferably, 10 mm to 40 mm away), and write/read operations are communicated from the reader to the smartcard. The reader then compares the scanned biometric data and stored biometric data to determine if there is a match. The reader may be located at an access point to provide access to a location or equipment in a security system dependent on the results of the comparison. An encoder is able to perform the functions of a reader including contactless communications with the smartcard, but also is able to encode a smartcard with personal details and biometric data. More particularly, the encoder preferably includes a logical access system where all access in a facility is controlled using a card, i.e. for doors, for PC access, etc. Such a smartcard access system by its nature almost ensures that the user does not forget to leave the smartcard behind. Preferably, an encoder has an appropriate interface to enable the encoder to be connected with a computer to enrol a person's details and biometric data on the smartcard using software running on the computer. The encoder stores biometric data in a two-dimensional structure or template and card holder details on the smartcard. The encoder may have an insert slot in the housing body to receive such a smartcard. The slot allows detection of the smartcard during an encoding process. A reader cannot be used for enrolment of biometric data and other associated information on a smartcard as can an encoder. For ease of description, the following text uses the two terms biometric smartcard reader and biometric smartcard encoder substantially interchangeably, but the noted distinctions should be borne in mind.

Biometric Smartcard Reader or Encoder

In accordance with an embodiment of the invention, a biometric smartcard reader or encoder is disclosed. Fig. 5 is a block diagram illustrating a smartcard 540 and a biometric smartcard reader 500 in accordance with an embodiment of the invention. This biometric smartcard reader 500 is smaller than other biometric units. The biometric smartcard reader 500 includes a biometric sensor 510 coupled to a sensor control module or printed circuit board 520. The sensor PCB 520 contains modules for processing and encoding scanned biometric data into a suitable digital representation using a given

coding algorithm (e.g., Sagem). The fingerprint is stored as a template preferably and not as a digital image. An algorithm is used to generate the template. For fingerprints, examples of relevant algorithms use minutiae reference points, or ridge recognition patterns, for example. In turn, the sensor PCB 520 is coupled to a smartcard reader PCB 530 and sends fingerprint data in a given template to the smartcard reader PCB 530, which is also able to interrogate and obtain data from a smartcard 540. This is preferably done by presenting the smartcard reader PCB 530 with the smartcard 540, in which the smartcard reader PCB 530 energises the smartcard 540 if in close proximity and communicates with the smartcard 540. Preferably, the smartcard reader PCB 530 is a contactless reader using a Philips Chip Mifare® utilising the Wiegand format for its output. Communication between the smartcard 540 and the smartcard reader PCB 530 is encrypted. The encryption utilised with this embodiment involves a proprietary encryption method of Mifare®, which is embedded in the Mifare® smartcards. Another option is to use DES encryption. However, it will be apparent to those skilled in the art in the light of this disclosure that other encryption techniques may be used without departing from the scope and spirit of the invention.

More preferably, the biometric smartcard reader 500 incorporates a biometric finger scan sensor 510 (e.g., for scanning fingerprints) with an accompanying sensor PCB 520. The fingerprint sensor technology may be optical, capacitive, thermal, tactile, or a combination of the foregoing. An example of a sensor arrangement that may be used is a Bioscrypt product provided by Bioscrypt Inc. including an Authentic sensor, a Bioscrypt PCB, and Bioscrypt's own encoding algorithm. Alternatively, the sensor arrangement may be implemented using an ST sensor, a Yuean PCB provided by Yuean Biometrics, and the Sagem algorithm, or a SecuGen product provided by SecuGen Corporation including a SecuGen sensor, a SecuGen PCB, and the SecuGen algorithm. Still further, a SecuGen optical solution may be practiced that enables a rugged and robust design. However, it will be apparent to those skilled in the art in the light of this disclosure that other biometric sensors may be practiced without departing from the scope and spirit of the invention. The sensor 510 and associated PCB 520 scan a person's fingerprint and generate a digital representation of that fingerprint as digital biometric data. Fig. 6 is a perspective view of a biometric smartcard reader 600, which embodies the reader 500 of

Fig. 5 including a biometric sensor 610/510, an associated sensor PCB 520 (not shown), and a Mifare® smartcard reader PCB 530 (not shown) in a single unit.

The smartcard 540 is adapted to store a digital representation of the biometric data. Preferably, the smartcard is a Mifare® smartcard for use with the contactless Mifare® reader. The smartcard 540 has approximately 1 Kbyte of storage or memory. Fig. 4A is a block diagram illustrating the structure of the storage 400 in the Mifare® smartcard, which is organised into 16 separate sectors 410-414 – 0 sector 410, 1 sector 412, ..., 15 sector 414. Each of the sectors 410-414 has two keys, Key A and Key B as shown in Fig. 4B. These keys can be designated as read and read/write keys. The keys A and B for each sector are initialised by the manufacturer (e.g. 10 hexadecimal characters each) and can be changed when the sectors are written to to contain biometric data in accordance with the embodiment of the invention. Each Mifare® smartcard 540 also has a unique serial number or identifier. Preferably, the 15th sector 414 contains one or more of the following security parameters for use in the system of Fig. 5: a facility code, a company code, an access code, and an issue code. The facility code can identify a facility that the smartcard permits access to for a given entity or company, which is identified by the company code. The issue code identifies how many smartcards have been issued to a person. For example, if the issue code is 3, the system may hotlist corresponding smartcards for the person with issue codes of 1 or 2.

Dependent upon the format of the digital biometric data, the smartcard 540 stores such data across two or more sectors with corresponding keys for each sector of data. In the preferred embodiment, 5 to 6 sectors are used to store a digital fingerprint representation or template. For example, an ST sensor and an Yuean PCB produces a digital fingerprint representation that is approximately 320 bytes long. The length of the representation may vary depending on the different biometric sensor products and algorithms used. As noted above, each sector needs a customer specific key to unlock the information.

Optionally, the reader 500/600 incorporates a tamper switch so that if a reader is pulled from a wall, the reader does not function and an alarm flag is activated.

As described in greater detail below, use of the biometrics smartcard encoder 500 enables authorised persons using a properly enrolled smartcard to access to a secure location or equipment, for example. Lost or stolen smartcards 540 are unusable as the person with the lost or stolen smartcard 540 does not have the correct biometrics data (e.g., fingerprint) to match that stored on the smartcard 540. Still further, another advantage of this embodiment is that the biometric smartcard reader 500 of Fig. 5 obviates the need for a central database or repository of biometric data, since the biometrics data is stored on the smartcard 540.

In combination with a computer (not shown), a biometrics smartcard encoder 500 can also be used to enrol a person's fingerprint on a smartcard 540. The biometrics smartcard encoder 500 uses an RS232 or USB communications port, in conjunction with software, to enrol the person's fingerprint onto the smartcard 540. Generally, software or a computer program(s) running on the computer in combination with the biometrics smartcard encoder 500 obtains personal details for a person, scans and records a fingerprint for the person, and then writes the personal details and fingerprint representation to the smartcard 540. Preferably, this embodiment does not permit fingerprint information to travel to the computer. Instead, the biometric smartcard encoder 500 stores the information and writes the information directly to the smartcard 540. The information is then erased from the memory of the biometric smartcard encoder 500. When enrolling a person's fingerprint, the detail level for scanning by the biometric smartcard encoder 500 can be changed to enable persons with scarred hands or other aberrations to use the encoder 500. This process is set forth in greater detail with reference to Fig. 1.

Fig. 1 is a high-level flow diagram illustrating details of a process 100 of obtaining and storing biometric information in a smartcard 540 using the biometric smartcard encoder (i.e., biometric unit) 500/600. In state 110, the biometric smartcard encoder 500 is initially idle. In step 112, a command is sent to the biometric smartcard encoder 500 to capture a person's fingerprint. This is preferably done by the computer using a communications port. In step 114, the sensor 510/610 of the biometric smartcard encoder 500 captures a fingerprint image. The sensor 510/610 analyses the scanned fingerprint and creates an image. In step 116, the image is coded and the data to be stored

is created. This is preferably done by the sensor PCB 520 in combination with the sensor 510. In step 118, the smartcard 540 is presented to the smartcard reader PCB 530, and the biometric data from the sensor PCB 520 is written into the smartcard 540 by the smartcard reader PCB 530. State 120 at the end of the process 100 shows that the digital fingerprint representation is stored on the smartcard 540. This smartcard 540 can then be used as a security key in relation to a biometric security system.

Generally, when verification or access is required using a biometric smartcard reader 500/600, the smartcard 540 is presented to the biometric smartcard reader 500/600 and the fingerprint information is read off the smartcard 540 by the biometric smartcard reader 500/600. The person then presents their finger to the sensor 510/610 of the biometric smartcard reader 500/600 for scanning. The fingerprint representation read off the smartcard 540 is compared by the biometric smartcard reader 500/600 with the fingerprint currently obtained using the sensor 510/610. If there is a match within the detail level set at enrolment, the biometric smartcard reader 500/600 checks access privileges using the access code from the smartcard 540 and if the holder has appropriate access privileges, access is granted by the biometric smartcard reader 500/600 to the smartcard holder. Verification is strongly dependent on enrolment. A score of 100 applies for a high quality and content template. A medium threshold level may look for a score of 60, for example. The threshold level may be varied to adjust quality and content of a template.

Details of Enrolment Process

Fig. 2 is a more detailed flow diagram of a process 200 of enrolling a fingerprint using a biometric smartcard encoder, based on Fig. 1. In an initial state 210, a biometric software application is run or launched. As noted above, this software is run on a computer connected to a biometric smartcard encoder 500/600, preferably using a RS232 or USB communications port. In step 212, a relevant RS232 or USB port (denoted generally by COM in Fig. 2) is selected by the software. Other interfaces may be practiced without departing from the scope and spirit of the invention. In step 214, the communications link (COM port) is tested to ensure the communications link is operating properly. Communication between the smartcard reader PCB 530 and the computer is preferably triple DES or Skipjack encrypted. Therefore, the information sent for access to

the computer is highly difficult to compromise. In step 216, enrolment of a person's fingerprint is commenced. Preferably, this is done by clicking on an enrolment tab in the software application to commence enrolment processing. In step 218, personal details of the person whose fingerprint is to be enrolled are obtained and the type of smartcard being written to is specified. The relevant information may include one or more of the person's name, facility code, company code, access code, and issue code. Alternatively, the smartcard may be pre-encoded with some or all of this information.

In step 220, the desired detail level of the fingerprint is specified using the software application. In particular, this is done using a quality meter in the software where the detail level for the sensor 510 and PCB 520 is specified. Ordinarily, the quality is set as high as possible to avoid misreads. However, the quality can be adjusted downwardly to avoid or reduce the effects of scar tissue and other aberrations on the person's finger. In step 222, the person's fingerprint is presented to the sensor 510/610 of the biometric smartcard encoder 500/600, and the person's fingerprint is scanned. The data stream for the scanned fingerprint is sent from the sensor 510/610 to the sensor PCB 520. The information is then coded with the specific algorithm within the sensor PCB 520. The coded information is then sent to the smartcard reader PCB 530 and from there encoded onto the smartcard 540.

In decision block 224, a check is made to determine if the quality of the scanned fingerprint image from the sensor 510/610 is adequate. The sensor 510 and PCB 520 determines quality. The biometric smartcard encoder 500/600 indicates this to the computer, since the fingerprint is preferably not transferred to the computer. If the quality is inadequate (NO), the quality is reduced to enable enrolment in step 226 and processing continues at step 222. This may occur multiple times. If decision block 224 determines that the quality is adequate (YES), processing continues at step 228.

In step 228, a smartcard 540 is presented to the smartcard reader PCB 530 of the biometric smartcard encoder 500/600. Presentation of the smartcard 540 to the smartcard reader PCB 530 results in the encoded fingerprint template and related keys for each sector being downloaded onto the smartcard 540. The communication between the smartcard 540 and the reader PCB 530 is encrypted. As noted above, the encrypted,

encoded fingerprint representation is normally stored across several sectors in the storage of the smartcard. Also personal details and other information may be stored on the smartcard 540. In step 230, a check is made to determine if the encoding of the smartcard 540 was successful. If decision block 230 returns true (YES), the fingerprint template has been encoded successfully on the smartcard 540 using the encoder 500. If decision block 230 returns false (NO), processing continues at decision block 232. In decision block 232, a check is made to determine if the smartcard type details are correct. For example, the smartcard 540 may be a new or used smartcard. A new smartcard has default values in its storage, while a used smartcard has changed keys A and B for example. Further, or alternatively, a different type of smartcard may be used, for example, from different manufacturers. If decision block 232 returns false (NO) indicating the card type details are incorrect, processing continues at step 234 and the correct smartcard type must be specified to the software. Processing then continues at step 236. If decision block 232 returns true (YES), processing continues at step 236. In step 236, another smartcard is tried or obtained for presentation instead of the smartcard previously presented to the smartcard reader PCB 530 of the encoder 500/600. Processing then continues at step 228.

Details of Verification Process

After a fingerprint representation and associated information are enrolled on a smartcard 540, verification of the enrolment on the smartcard 540 may be required. Fig. 3 is a flow diagram illustrating a process 300 of verifying a fingerprint scanned by the biometric smartcard encoder 500/600 and enrolled on the smartcard 540. In state 310, the biometric application software is loaded. In step 312, the communications link (COM port or USB) between the computer and the biometric smartcard encoder 500 is selected. In step 314, the communications link is tested to ensure the link is operating properly. In step 316, a verification application module in the software is activated. Preferably, this is done by clicking on a verify tab in the biometric application software. In step 318, the smartcard 540 with enrolled fingerprint information is presented to the encoder 500/600, which reads and stores the fingerprint information from the smartcard 540. In step 320, the person's finger is presented to sensor 510/610 of the biometric smartcard encoder 500, and the person's fingerprint is scanned and stored. The biometric smartcard encoder 500 then compares in the smartcard reader PCB 530 the scanned fingerprint template from the sensor 510/610 and the uploaded fingerprint template from the smartcard 540.

In decision block 322, a check is made to determine if the verification passed (OK). The encoder 500/600 provides the comparison result to the computer to establish verification. If decision block 322 returns true (YES), processing continues at state 324 and the fingerprint on the smartcard is verified as that of the fingerprint obtained at the sensor 510/610. Otherwise, if decision block 322 returns false (NO), processing continues at step 326. In step 326, a check is made to determine if the verification bar in the software was raised. Preferably, a quality bar and a verification bar showing current levels are depicted graphically to an operator of the application software on opposite sides of a graphical image of a fingerprint icon, which indicates to the operator when a fingerprint has been properly scanned by the encoder 500/600. Raising the verification bar indicates a better match between the scanned fingerprint and the one from the smartcard 540. Verification is dependent on the quality level at enrolment. If decision block 326 returns true (YES), processing continues at step 332 and the finger must be positioned correctly for verification, before processing continues at step 320. Otherwise, if decision block 326 returns false (NO), processing continues at step 328. A determination is made that the incorrect finger has been used in relation to the recorded fingerprint information on the smartcard. In step 330, the correct finger is determined before proceeding to step 320.

Secure Transmission System

In a security system, a smartcard reader may be setup to give access on a per door basis or to equipment. The smartcard has unique keys that must also be contained in a smartcard reader's firmware. The smartcard reader communicates with the smartcard and information is read from the smartcard for access. The smartcard reader ordinarily communicates with an access controller, and this controller controls access; for example the controller may preferably activate a door latch for access. Information is sent to the controller. Communication between the smartcard reader and the controller is usually Wiegand. However, the communications may be RS485 or RS232. Still further, another example of a common form of communication back to a controller is Clock and Data. These formats can be cracked or defeated given time, as formats are usually 'known' industry standards. The controller determines whether or not to grant access and activates an access mechanism if granted. When using a security access reader to grant or deny

access, a possible breach in security lies in the information that is directly sent to the controller by the smartcard reader. If the smartcard reader is removed from a wall or other connection point and a signal is introduced to the line between the smartcard reader and the controller, then a security breach exists. The signal may provide information to the controller so that the controller improperly grants access. If the smartcard reader has a tamper switch, a degree of added security is provided. A hole in the wall may still be made conditional to the material of the wall, and a security breach may still occur, as this enables access to the cables of the reader. In contrast, a stand-alone reader does not need a controller so this does not apply to such a reader.

In accordance with a further embodiment of the invention, secure transmission from a smartcard reader is provided by encrypting the messages from the smartcard reader in the security system. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The further embodiment of the invention shown in Figs. 7 and 8 addresses this issue.

Fig. 7 is a block diagram of a secure transmission system 700 in accordance with the further embodiment of the invention. A smartcard reader 702 is coupled to a high security module (HSM) 704. Preferably, the smartcard reader 702 is a biometrics smartcard reader 500/600, but may be a standard smartcard reader. The HSM 704 is located remotely from the smartcard reader 702 and preferably at an inaccessible location relative to the smartcard reader 702, for example on the other side of a wall in a secure area. The distance between the smartcard reader 702 and the HSM 704 may be up to 15 metres. Communications between the reader 702 and the HSM 704 are preferably Triple DES or Skipjack encrypted, but other encryption techniques may be employed. The HSM 704 is in turn coupled to a controller 706. Communications between the HSM 704 and the controller 706 are carried out using the controller-specified format, which is usually Wiegand format but may be another format (e.g., clock and data). In turn, the controller 708 is connected to the door latch 708 to control operation of the door for access. Different access mechanisms may be used in place of a door latch 708, for example to provide access to a computer.

Significantly, the system 700 uses an HSM 704 for each access point and encrypted communications between the smartcard reader 702 and the HSM 704. The smartcard reader 702 preferably reads the information off a smartcard and communicates with the HSM 704 on the secure side of the wall, up to 15 metres away. Again, the communication is encrypted, preferably using a 3DES or Skipjack encrypted protocol. The HSM 704 decrypts the message to obtain the security information from the smartcard, e.g. "Facility Code" and the "Access number", and communicates these values to the access controller 706. Thus, communication between the smartcard reader 702 and the HSM 704 and thus the controller 706 is secure whether the smartcard reader 702 is removed from the wall or wiring is accessed through a wall. This provides a higher standard of security for access control systems.

Fig. 8 is a flow diagram illustrating a process 800 for secure transmission. In state 810, the smartcard reader 702 is in standby mode. In step 812, a smartcard is presented for access. In step 814, the smartcard reader 702 reads and analyses access information on the smartcard. The smartcard and the reader must have the same keys. If a standard smartcard reader is used, an encrypted transmission is sent to the HSM 704 in step 816. Processing then continues at step 824. Otherwise, if a biometric smartcard reader 500/600 is used, after step 814, processing continues at step 818. In step 818, biometric data is obtained from the cardholder using the biometric sensor of the biometric smartcard reader 500/600 as reader 702. Preferably, the biometric data is fingerprint information. In step 820, the biometric data of the cardholder and the stored biometric data from the smartcard are compared and confirmed to be the same person or not. If the biometric data matches, in step 822, an encrypted transmission for access is sent to the HSM 704 from smartcard reader 702, before processing continues at step 824. In step 824, the HSM 704 decrypts the transmission and communicates it to the controller 706 using the appropriate controller format, e.g. Wiegand. The controller 706 either grants access 828 in step 826 or denies access 832 in step 830 dependent upon the access rights obtained from the smartcard.

A small number of embodiments of the invention regarding methods, devices, and systems for biometric smartcard reading and encoding, as well as for secure transmissions have been described. In the light of the foregoing, it will be apparent to

those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention.

Claims

The claims defining the invention are as follows:

1. A method of identification using biometric data, said method including the steps of:

reading a smartcard encoded with biometric data;

sensing actual biometric data;

comparing said biometric data from said smartcard with said sensed biometric data identification.

2. The method according to claim 1, further including the step of allowing access if said biometric data from said smartcard and said obtained biometric data match.

3. The method according to claim 1, further including the step of verifying said biometric data encoded on said smartcard is correct.

4. The method according to claim 1, further including the step of enrolling biometric data on said smartcard.

5. The method according to claim 4, wherein said enrolling step further includes the steps of:

scanning a source of biometric data associated with said smartcard;

encoding said scanned biometric data; and

storing said encoded biometric data on said smartcard.

6. The method according to claim 1 or 5, wherein said biometric data includes a fingerprint.

7. The method according to claim 5, further including the step of specifying a detail level for scanning said biometric data.

8. An apparatus for identification using biometric data, said apparatus including:

means for reading a smartcard encoded with biometric data;

means for sensing actual biometric data;

means for comparing said biometric data from said smartcard with said sensed biometric data.

9. The apparatus according to claim 8, further including means for allowing access if said biometric data from said smartcard and said biometric data obtained at said access point match.

10. The apparatus according to claim 8, further including means for verifying said biometric data encoded on said smartcard is correct.

11. The apparatus according to claim 8, further including means for enrolling biometric data on said smartcard.

12. The apparatus according to claim 11, wherein said enrolling means further includes:

a biometric scanner for scanning a source of biometric data associated with said smartcard;

means for encoding said scanned biometric data; and

a smartcard reader for storing said encoded biometric data on said smartcard.

13. The apparatus according to claim 8 or 12, wherein said biometric data includes a fingerprint.

14. The apparatus according to claim 12, further including means for specifying a detail level for scanning said biometric data.

15. A method of providing secure transmissions from a smartcard reader, said method including the steps of:

encrypting a signal created by said smartcard reader dependent on said smartcard;

transmitting said encrypted signal to a remote location relative to said reader;

translating at said remote location said transmitted signal to another format usable by a controller;

controlling access using said controller dependent upon said translated signal.

16. The method according to claim 15, wherein said smartcard contains biometric data and said smartcard reader includes a biometric smartcard reader for obtaining biometric data directly.

17. The method according to claim 16, wherein said biometric data includes fingerprint data.

18. An apparatus for providing secure transmissions from a smartcard reader, said apparatus including:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard;

means for transmitting said encrypted signal to a remote location relative to said smartcard reader;

means for translating at said remote location said transmitted signal to another format;

a controller for controlling access using dependent upon said translated signal.

19. The apparatus according to claim 18, wherein said smartcard contains biometric data and said smartcard reader includes a biometric smartcard reader for obtaining biometric data directly.

20. The apparatus according to claim 19, wherein said biometric data includes fingerprint data.

BIOMETRIC SMARTCARD SYSTEM AND METHOD OF SECURE TRANSMISSION

Abstract

Secure transmission systems and security systems utilising biometric sensors are disclosed. A smartcard encoded with details of biometric data is read, and actual biometric data is sensed. The biometric data from the smartcard is then compared with the sensed biometric data. Access may be allowed if the biometric data from the smartcard and the sensed biometric data match. The process may involve verifying the biometric data encoded on the smartcard is correct. The smartcard stores the biometric data after a source of biometric data is scanned and the scanned biometric data is encoded. In a further aspect, secure transmissions are enabled from a smartcard reader. To do so, a signal obtained by the reader dependent on the smartcard is encrypted. The encrypted signal is transmitted to a remote location relative to the reader. At the remote location, the transmitted signal is translated to another format usable by a controller. Access is controlled by the controller dependent upon the translated signal.

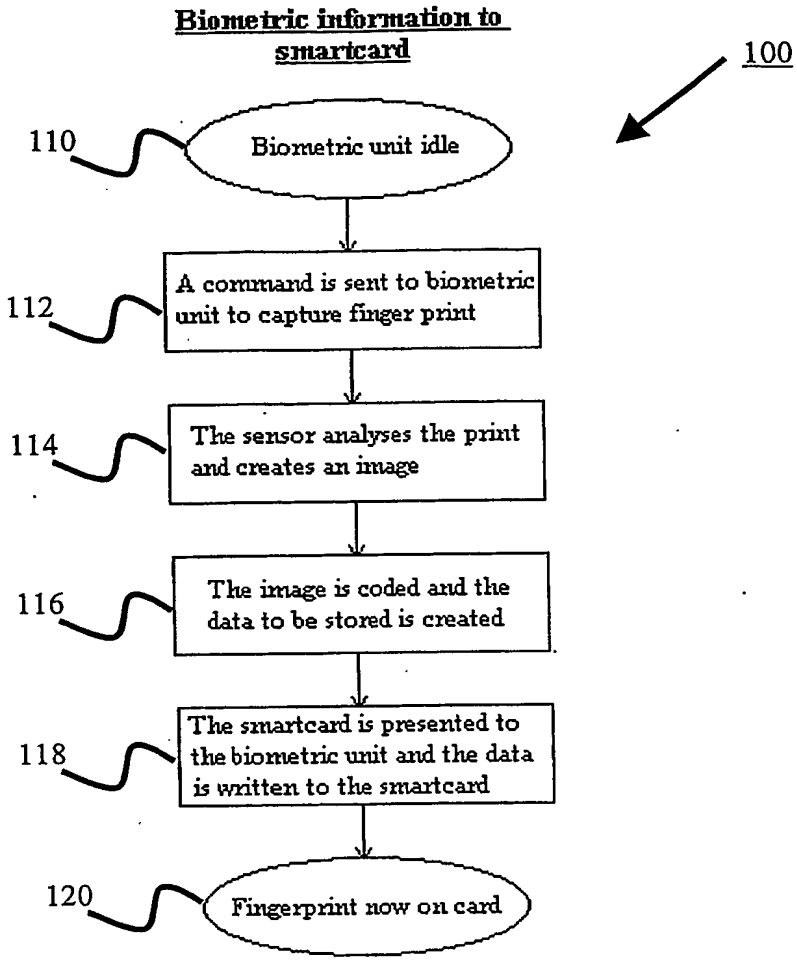
Biometric information to smartcard
100
110
Biometric unit idle
112
A command is sent to biometric unit to capture finger print
114
The sensor analyses the print and creates an image
116
The image is coded and the data to be stored is created
118
The smartcard is presented to the biometric unit and the data is written to the smartcard
120
Fingerprint now on card

FIG. 1

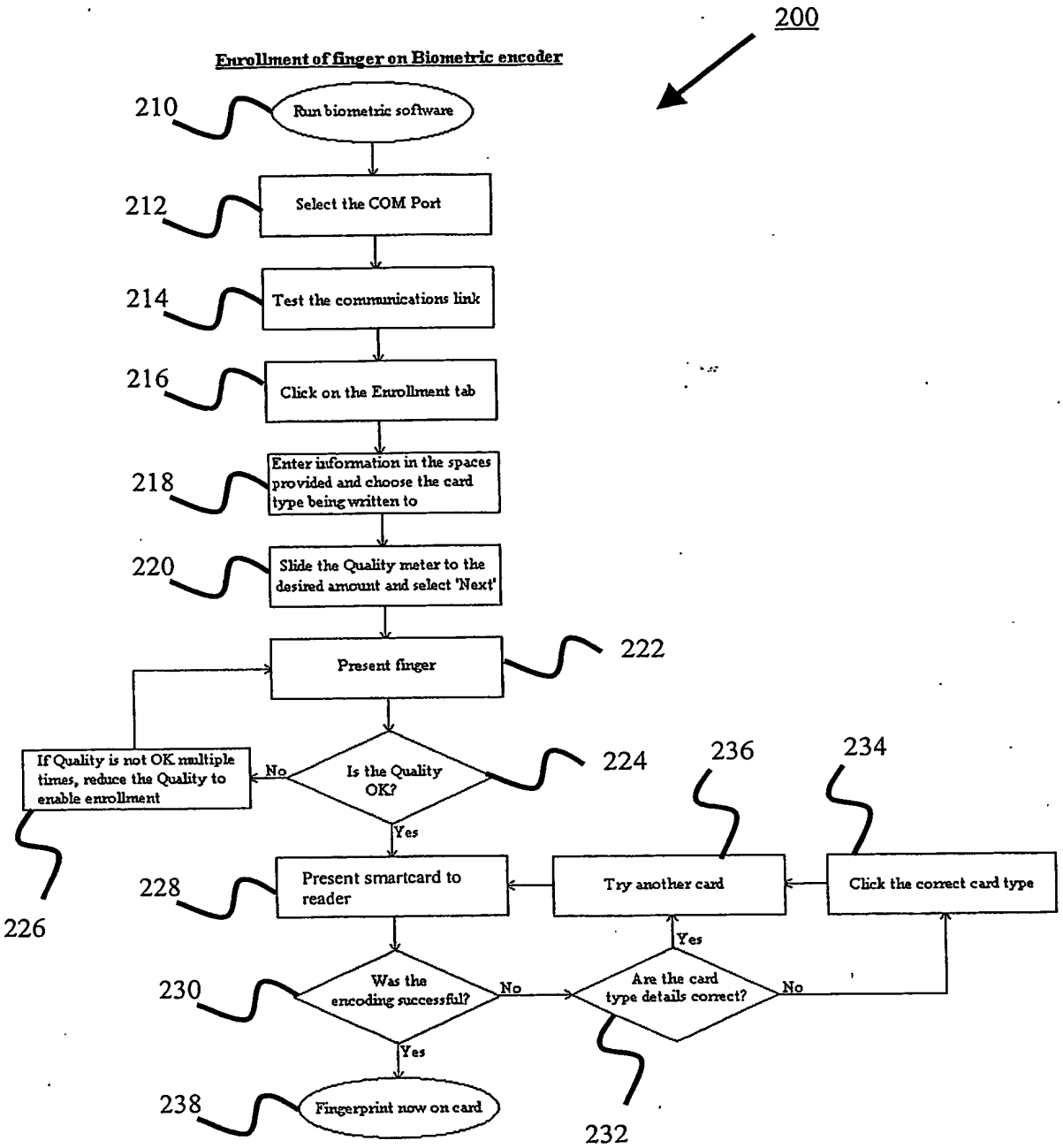
200
Enrollment of finger on Biometric encoder
210
Run biometric software
212
Select the COM Port
214
Test the communications link
216
Click on the Enrollment tab
218
Enter information in the spaces provided and choose the card type being written to
220
Slide the Quality meter to the desired amount and select 'Next'
Present finger
222
If Quality is not OK multiple times, reduce the Quality to enable enrollment
No
Is the Quality OK?
224
Yes
226
228
Present smartcard to reader
Try another card
236
Click the correct card type
234
Yes
230
Was the encoding successful?
No
Are the card type details correct?
No
Yes
232
238
Fingerprint now on card

FIG. 2

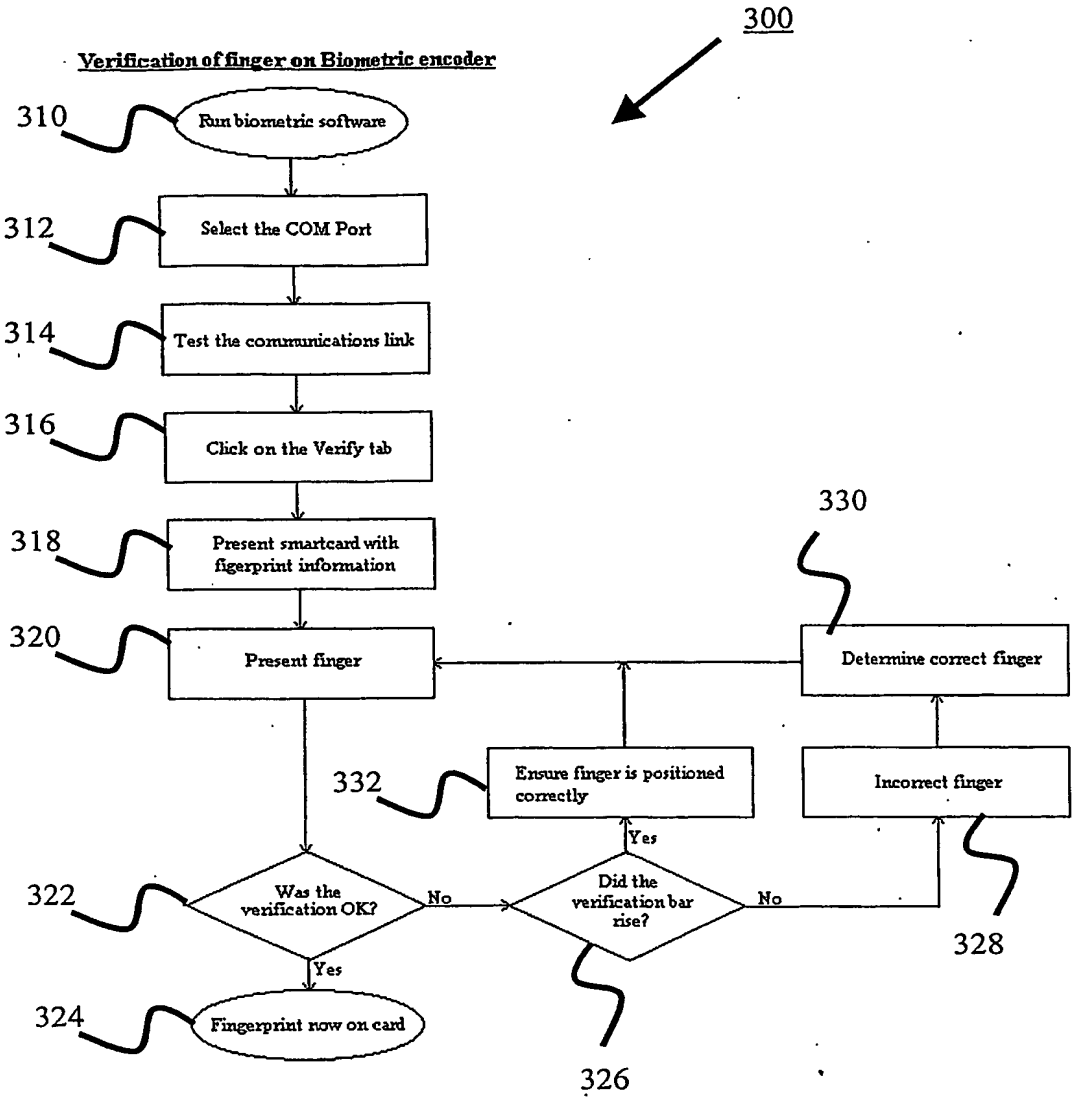
300
Verification of finger on Biometric encoder
310
Run biometric software
312
Select the COM Port
314
Test the communications link
316
Click on the Verify tab
318
Present smartcard with figerprint information
320
Present finger
330
Determine correct finger
332
Ensure finger is positioned correctly
Incorrect finger
Yes
322
Was the verification OK?
No
Did the verification bar rise?
No
328
Yes
324
Fingerprint now on card
326

FIG. 3

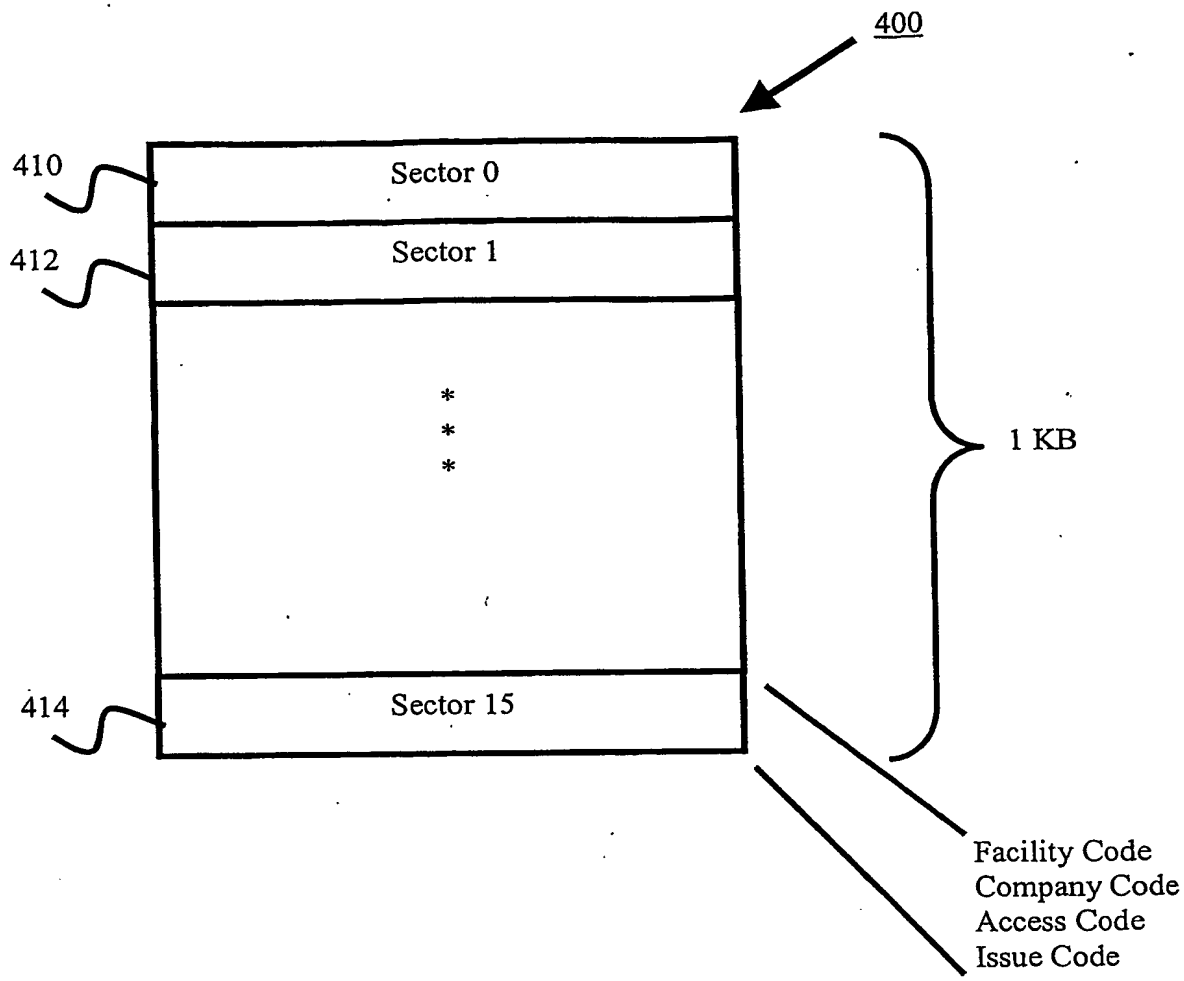

FIG. 4A

450

Sector	Key A	Key B
0	A0A1A2A3A4	-
	or	
	FFFFFFFFFF	-
*		
*		
*		
15		

FIG. 4B

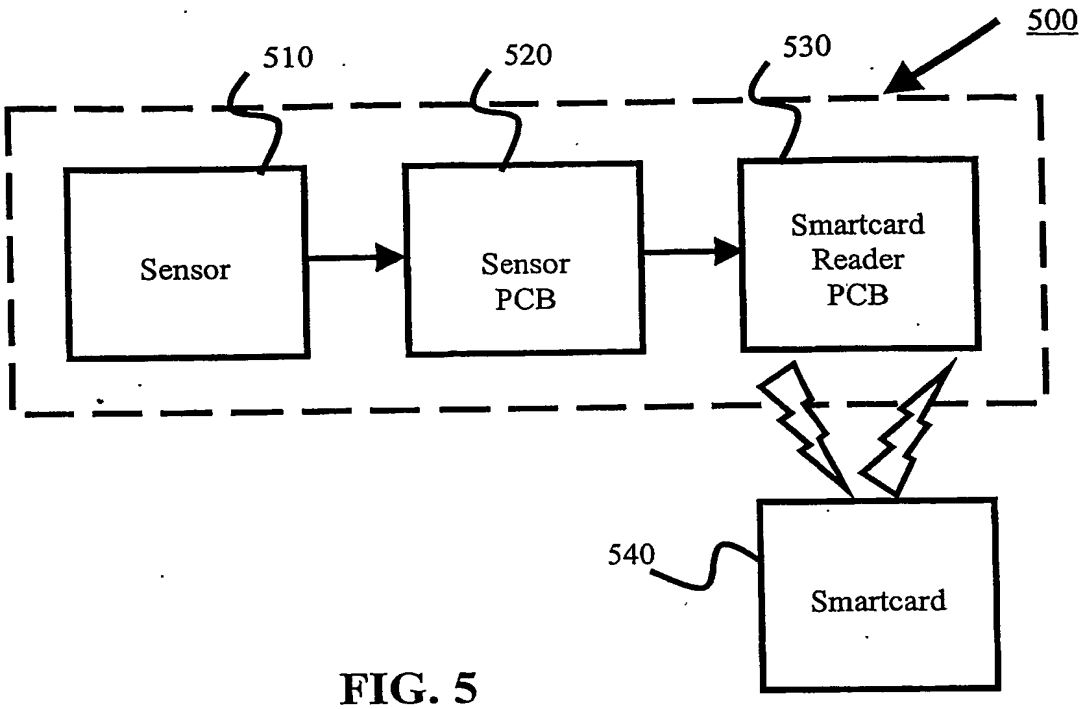
500
510
520
530
Sensor
Sensor PCB
Smartcard Reader PCB
540
Smartcard

FIG. 5

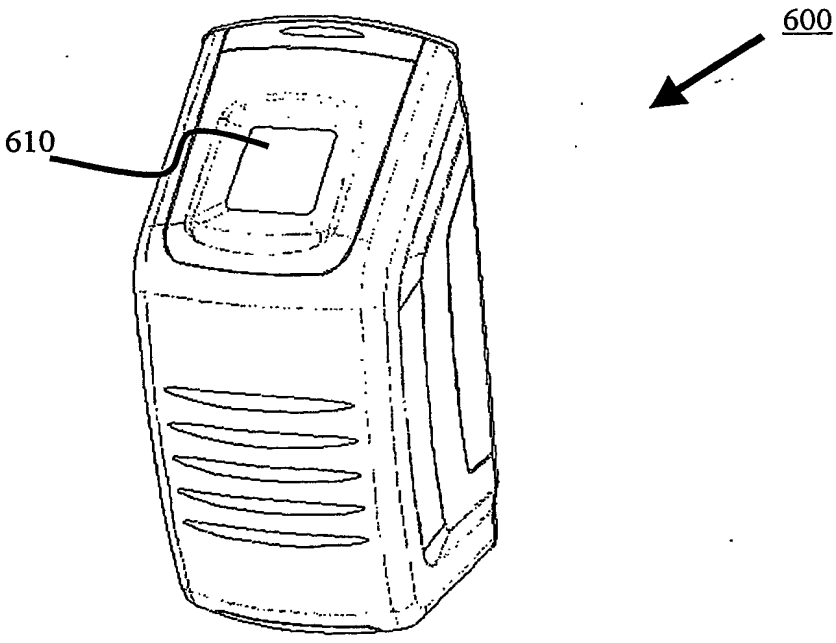
600
610

FIG. 6

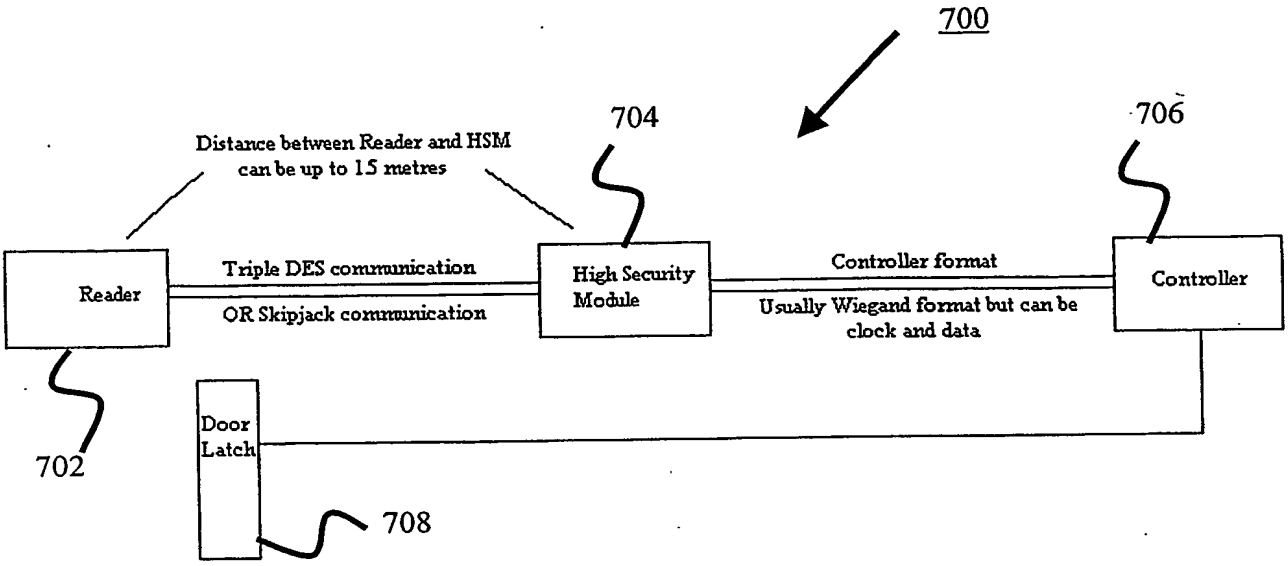
700
704
706
Distance between Reader and HSM
can be up to 15 metres
Reader
Triple DES communication
OR Skipjack communication
High Security
Module
Controller format
Usually Wiegand format but can be
clock and data
Controller
Door
Latch
702
708

FIG. 7

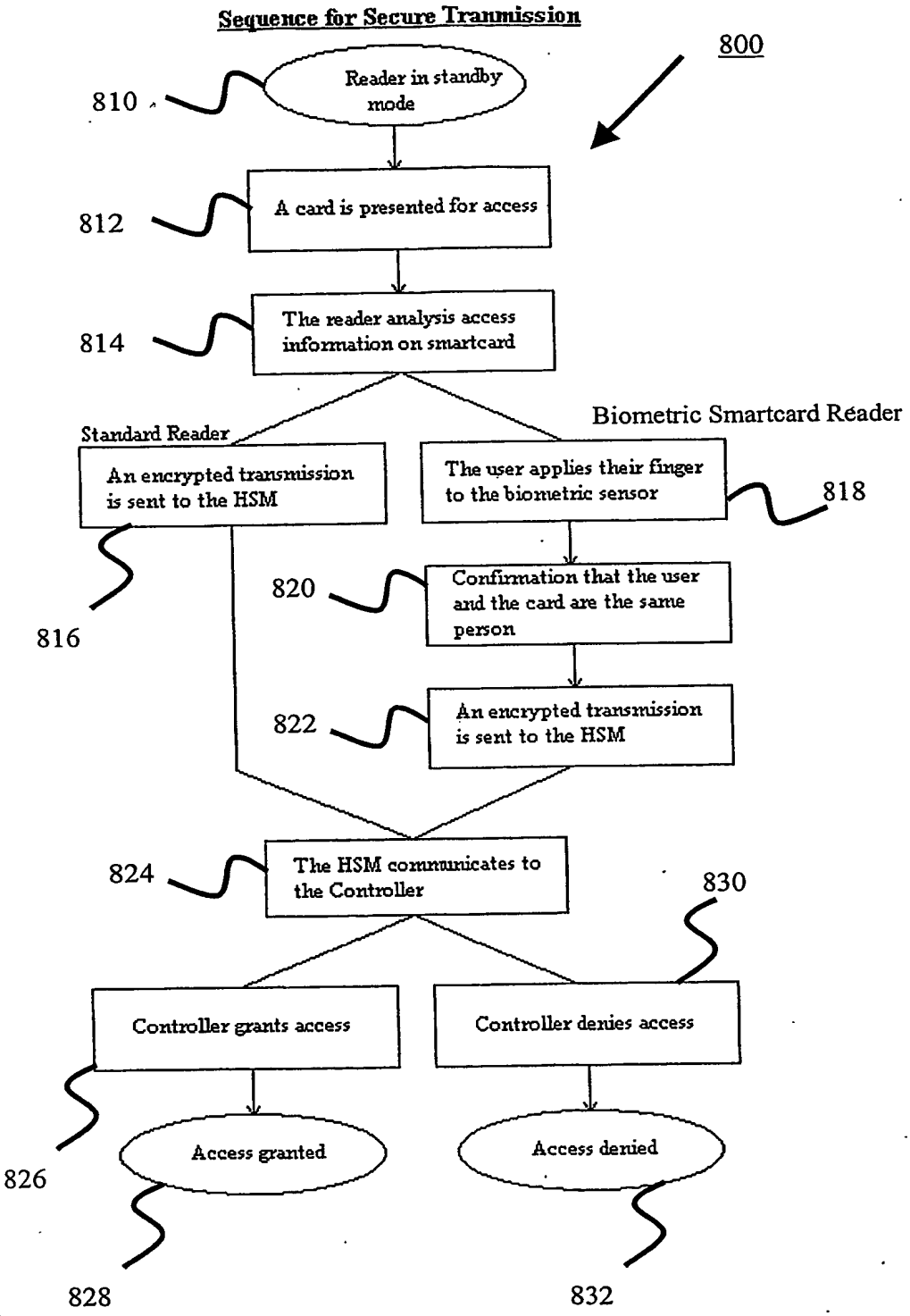
Sequence for Secure Transmission
800
Reader in standby mode
810
A card is presented for access
812
The reader analysis access information on smartcard
814
Standard Reader
Biometric Smartcard Reader
An encrypted transmission is sent to the HSM
The user applies their finger to the biometric sensor
818
816
820
Confirmation that the user and the card are the same person
822
An encrypted transmission is sent to the HSM
824
The HSM communicates to the Controller
830
Controller grants access
Controller denies access
826
Access granted
Access denied
828
832

FIG. 8

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☑ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.